

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
127 2nd St., Gold Bar, Washington (SUBJECT
PREMISES)

Case No. MJ19-025

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched, and give its location):
The Subject Premises as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

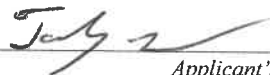
The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C. § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

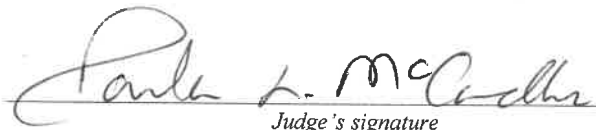
SPECIAL AGENT TOBY LEDGERWOOD, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 1-17-19

City and state: BELLINGHAM, WASHINGTON



Judge's signature

PAULA L. MCCANDLIS, U.S. MAGISTRATE JUDGE

Printed name and title

ATTACHMENT A

Description of Property to be Searched

The SUBJECT PREMISES is the property located at 127 2nd St., Gold Bar, Washington, and is more fully described as a parcel containing a single family house with a basement. The house has white colored siding with white trim around the windows. There is a black mailbox posted in front of the house with the numbers 127 affixed in black lettering with a white background. There are multiple security cameras affixed to the house as well as the entry posts.

The search is to include all rooms within the SUBJECT PREMISES, all persons and vehicles on the SUBJECT PREMISES, all garages, outbuildings, or storage units, attached or detached, and any digital device(s) found therein.

ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media.

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography or evidencing contact with minors;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

- a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;
- b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;
- c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;
- d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;
- e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;
- f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
- g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;
8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;
9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;
10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

1 11. Evidence of counter-forensic programs (and associated data) that are
2 designed to eliminate data from a digital device;

3 12. Evidence of times the digital device(s) was used;

4 13. Any other ESI from the digital device(s) necessary to understand how the
5 digital device was used, the purpose of its use, who used it, and when.

6 14. Records and things evidencing the use of the IP address 67.183.169.49 (the
7 SUBJECT IP ADDRESS) including:

8 a. Routers, modems, and network equipment used to connect
9 computers to the Internet;

10 b. Records of Internet Protocol (IP) addresses used;

11 c. Records of Internet activity, including firewall logs, caches, browser
12 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
13 entered into any Internet search engine, and records of user-typed web addresses.

14
15 **The seizure of digital devices and/or their components as set forth herein is**
16 **specifically authorized by this search warrant, not only to the extent that such**
17 **digital devices constitute instrumentalities of the criminal activity described above,**
18 **but also for the purpose of the conducting off-site examinations of their contents for**
19 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
20
21
22
23
24
25
26
27
28

AFFIDAVIT

STATE OF WASHINGTON)

) ss

COUNTY OF WHATCOM)

I, Toby Ledgerwood, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Assistant Special Agent in Charge (ASAC) Blaine, Washington, field office. I have been employed as an HSI Special Agent since 2006. Prior to this assignment, I worked as a United States Customs Inspector from 2002 to 2006. In my capacity as a Special Agent, I am responsible for conducting investigations into the numerous federal laws enforced by HSI. Since 2013, I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the unlawful production, importation, distribution, receipt, attempted receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC), HSI Special Agent Training Program, and have received further specialized training in investigating child pornography and child exploitation crimes. My training included courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search warrants. I have observed and reviewed thousands of examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of many search warrants which involved child exploitation and/or child pornography offenses and the search and seizure of computers and other digital devices. Further, I have served as the affiant on numerous search warrants and complaints relating to child exploitation investigations. I am a member of the Internet

1 Crimes Against Children (ICAC) Task Force in the Western District of Washington, and
2 work with other federal, state, and local law enforcement personnel in the investigation
3 and prosecution of crimes involving the sexual exploitation of children. I have attended
4 periodic seminars, meetings, and training. I attended the ICAC Undercover
5 Investigations Training Program in Alexandria, Virginia, in June 2014 regarding child
6 exploitation. I also attended the Crimes Against Children Conference in Dallas, Texas, in
7 August 2014, where I received training relating to child exploitation, including training in
8 the Ares Peer to Peer (P2P) file sharing program. In September 2015, I received training
9 in the Emule (P2P) file sharing program. In March 2017, I received training in the
10 Gigatribe (P2P) file sharing program. I received a Bachelor of Science degree in
11 Criminal Justice with a minor in Sociology from the University of Missouri-St. Louis.

12 2. I am submitting this affidavit in support of an application under Rule 41 of
13 the Federal Rules of Criminal Procedure for a warrant to search the residence located at
14 127 2nd St, Gold Bar, Washington 98251 (hereinafter the "SUBJECT PREMISES") and
15 any persons found inside the SUBJECT PREMISES, more fully described in Attachment
16 A, for the things specified in Attachment B to this Affidavit, for the reasons set forth
17 below. I also seek authority to examine digital devices or other electronic storage media.
18 The property to be searched is as follows:

19 a. 127 2nd, St, Gold Bar, Washington 98251 (the SUBJECT
20 PREMISES);

21 3. The warrant would authorize a search of the SUBJECT PREMISES and a
22 seizure and forensic examination of digital devices found therein, for the purpose of
23 identifying electronically stored data as particularly described in Attachment B, for
24 evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) (Receipt
25 or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of
26 Child Pornography).

27 4. The facts set forth in this Affidavit are based on my own personal
28 knowledge; knowledge obtained from other individuals during my participation in this

1 investigation, including other law enforcement officers; review of documents and records
 2 related to this investigation; communications with others who have personal knowledge
 3 of the events and circumstances described herein; and information gained through my
 4 training and experience.

5 5. Because this affidavit is submitted for the limited purpose of establishing
 6 probable cause in support of the application for a search warrant, it does not set forth
 7 each and every fact that I or others have learned during the course of this investigation. I
 8 have set forth only the facts that I believe are relevant to the determination of probable
 9 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §
 10 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B)
 11 (Possession of Child Pornography), will be found at the SUBJECT PREMISES.

12 6. Based on the discoveries I have made, as described below, I believe that
 13 someone at the SUBJECT PREMISES has used a computer to connect to an Internet
 14 Peer-to-Peer (P2P) file sharing program, via Internet Protocol (IP) address 67.183.169.49
 15 (hereinafter the "SUBJECT IP ADDRESS"), and distributed videos depicting child
 16 pornography. I further believe that computers and other digital devices containing
 17 evidence of child pornography will be located at the SUBJECT PREMISES.

18 II. DEFINITIONS

19 7. The following definitions apply to this Affidavit:

20 Internet Service Providers

21 a. "Internet Service Providers" (ISPs), as used herein, are commercial
 22 organizations that are in business to provide individuals and businesses access to the
 23 internet. ISPs provide a range of functions for their customers including access to the
 24 Internet, web hosting, email, remote storage, and co-location of computers and other
 25 communications equipment. ISPs can offer a range of options in providing access to the
 26 Internet including telephone based dial up, broadband based access via digital subscriber
 27 line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs
 28 typically charge a fee based upon the type of connection and volume of data, called

1 bandwidth, which the connection supports. Many ISPs assign each subscriber an account
2 name – a user name or screen name, an “email address,” an email mailbox, and a
3 personal password selected by the subscriber. By using a computer equipped with a
4 modem, the subscriber can establish communication with an ISP over a telephone line,
5 through a cable system or via satellite, and can access the Internet by using his or her
6 account name and personal password. ISPs maintain records pertaining to their
7 subscribers (regardless of whether those subscribers are individuals or entities). These
8 records may include account application information, subscriber and billing information,
9 account access information (often times in the form of log files), email communications,
10 information concerning content uploaded and/or stored on or via the ISP's servers.

11 Internet Protocol (IP) Addresses

12 b. “Internet Protocol address” or “IP address” refers to a unique
13 number used by a computer to access the Internet. An IP address looks like a series of
14 four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every
15 computer connected to the Internet must be assigned an IP address so that the Internet
16 traffic sent from, and directed to, that computer may be properly directed from its source
17 to its destination. Most ISPs control the range of IP addresses.

18 **III. PEER-TO-PEER (P2P) FILE SHARING**

19 8. Based on my training and experience, I know the following regarding Peer-
20 to-Peer (P2P) file sharing networks, P2P client software programs, and the eDonkey2000
21 (eD2k) P2P file sharing network:

22 9. P2P file sharing is a method of communication available to Internet users
23 through the use of special software programs. P2P file sharing programs allow groups of
24 computers using the same file sharing network and protocols to transfer digital files from
25 one computer system to another while connected to a network, usually on the Internet.
26 There are multiple types of P2P file sharing networks on the Internet. To connect to a
27 particular P2P file sharing network, a user first obtains a P2P client software program for
28 a particular P2P file sharing network, which can be downloaded from the Internet.

1 10. In general, P2P client software allows the user to set up file(s) on a
2 computer to be shared on a P2P file sharing network with other users running compatible
3 P2P client software. A user can also obtain files by opening the P2P client software on
4 the user's computer and conducting a keyword search for files that are of interest and
5 currently being shared on the P2P file sharing network. The results of the keyword
6 search are displayed to the user. The user then selects file(s) from the results that he
7 wishes to download. The download of a file is achieved through a direct connection
8 between the computer requesting the file and one or more computers on the same P2P
9 network containing the file.

10 11. A computer running P2P client software has an IP address assigned to it
11 while it is connected to the Internet. Investigators are able to see the IP address of any
12 computer system sharing files. Investigators can then search public records that are
13 available on the Internet to determine the specific ISP who has assigned that IP address to
14 that computer. ISP's maintain logs and records which reflect the specific IP addresses it
15 assigned to specific computers that connect to the Internet through that ISP at any given
16 moment. Based upon the IP address assigned to the computer sharing files, subscriber
17 information then can be obtained from the ISP which contains identifying information of
18 the individual to whom the account is registered.

19 12. Based on my training and experience, P2P file sharing networks, including
20 the eD2k network, are frequently used to trade digital files depicting child pornography,
21 including both image and video files.

22 IV. STATEMENT OF PROBABLE CAUSE

23 13. On August 11th and 13th, 2018, while acting in an undercover capacity, I
24 used a law enforcement version of eMule, a commonly used P2P file sharing program for
25 the eD2k file sharing network, to identify P2P users possessing and distributing image
26 and video files depicting child pornography. I used the law enforcement version of
27 eMule to download files depicting child pornography from a P2P user at IP address
28

1 67.183.169.49 (the SUBJECT IP ADDRESS). I downloaded numerous video files
2 containing suspected child pornography. Two video downloads are detailed below.

3 14. On August 11, 2018, between approximately 21:08 (UTC) and 21:41
4 (UTC), I used the law enforcement version of eMule to establish a single-source
5 connection with a P2P user at the SUBJECT IP ADDRESS, who was determined to be in
6 possession of a suspected child pornography video file entitled "Xxxxx Pthc Mossi 11Y,
7 Molested By Her Dad (Crying).mpg" (subject video file 1). The law enforcement version
8 of eMule initiated a download of the subject video file and successfully downloaded the
9 partial file from the user at the SUBJECT IP ADDRESS.

10 **Filename: Xxxxx Pthc Mossi 11Y, Molested By Her Dad (Crying).mpg**

11 This video, depicts a prepubescent female (hereinafter the "child victim"). The
12 video shows the child victim lying on her back completely nude. The child victim
13 is seen using her hand to masturbate. An adult male is lying next to her visible
14 from the chest down. The adult male is nude from the waist down. The adult
15 male is seen using his hand to rub the child's genitals. The child victim has no
16 visible pubic hair, is young in appearance, and lacks muscular and breast
17 development. The child victim is approximately 8-10 years old.

18 15. On August 13, 2018, between approximately 09:12 (UTC) and 11:53
19 (UTC), I used the law enforcement version of eMule to establish a single-source
20 connection with a P2P user at the SUBJECT IP ADDRESS, who was determined to be in
21 possession of a suspected child pornography video file entitled "Boyfuck – 4Yr Nati 02
22 Man Suck Fuck 7Yo Boy.avi" (subject video file 2). The law enforcement version of
23 eMule initiated a download of the subject video file and successfully downloaded the
24 partial file from the user at the SUBJECT IP ADDRESS.

25 **Filename: Boyfuck – 4Yr Nati 02 Man Suck Fuck 7Yo Boy.avi**

26 This video, depicts a prepubescent male (hereinafter the "child victim"). The
27 video shows the child victim sitting on a bed nude from the waist down. The
28 child victim is seen climbing onto an adult male who is nude from the waist
down. The adult male is seen performing oral sex on the child victim. The adult
male is seen masturbating continuously throughout the video. The child victim
has no visible pubic hair, is young in appearance, and lacks muscular
development. The child victim is approximately 6-8 years old.

1 16. A query of a publicly available database revealed the SUBJECT IP
2 ADDRESS belonged to ISP Comcast Communications.

3 17. On October 24, 2018, a Department of Homeland Security (DHS)
4 administrative summons' was submitted to Comcast requesting subscriber information
5 for the SUBJECT IP ADDRESS during the dates and times the subject video files were
6 downloaded.

7 18. On October 30, 2018, Comcast provided the requested information. During
8 the dates and times the subject video files were downloaded, the SUBJECT IP
9 ADDRESS was assigned to Brian DIAZ at the residence located at 127 2nd St., Gold Bar,
10 Washington (the SUBJECT PREMISES). Comcast reported the IP History of the
11 SUBJECT IP ADDRESS to have a lease grant date and time of July 26, 2018, at 04:06:11
12 UTC and a lease expiration of October 24, 2018, at 23:18:32 UTC. The SUBJECT IP
13 ADDRESS is leased to Brian DIAZ with account number ending in 1745.

14 19. On November 5, 2018, I conducted a criminal history search of DIAZ. The
15 search revealed that DIAZ has no previous arrests or convictions.

16 20. On December 7, 2018, I conducted records checks via the Washington
17 State Department of Licensing (DOL) and found that DIAZ has a driver's license
18 registered to the SUBJECT PREMISES.

19 21. On December 7, 2018, Intelligence Research Specialist (IRS) Jon Dallas
20 conducted records checks via the Washington State Department of Licensing (DOL) and
21 found that DIAZ has a driver's license and vehicles registered to the SUBJECT
22 PREMISES. DOL records also indicated an individual named Daniel Diaz had a driver
23 license and vehicles registered to the SUBJECT PREMISES. As of December 2018,
24 DIAZ still has a driver's license and vehicle registered to the SUBJECT PREMISES.

25 22. Records checks conducted via the Snohomish County Assessor's Office
26 revealed that Daniel Diaz owns the SUBJECT PREMISES. The SUBJECT PREMISES
27 is listed as a single family residence with a basement on the Assessor's web-site.
28

1 23. On December 12, 2018, at approximately 11:09 a.m., SA Miller and I
2 conducted surveillance of the SUBJECT PREMISES and saw the following vehicles
3 parked in front of the SUBJECT PREMISES: a white Ford pickup bearing Washington
4 State license plate C92975J and a Hyundai Elantra with plate BFU5609. Records checks
5 revealed that the vehicles are registered to Daniel Diaz at the SUBJECT PREMISES.

6 24. On December 12, 2018, SA Miller and I installed a surveillance camera
7 across the street from the SUBJECT PREMISES. The camera was left in place from
8 December 12-17, 2018. A cursory review of the footage for the five days revealed the
9 vehicles registered to Daniel DIAZ regularly coming and going from the SUBJECT
10 PREMISES. No vehicles registered to Brian DIAZ were observed. Only one other
11 vehicle was observed during this five day period and it did not belong to either Daniel or
12 Brian DIAZ. The vehicle mentioned above arrived at the residence and departed after
13 approximately a few hours on December 12, 2018, and was not seen again.

14 25. On December 12, 2018, while conducting surveillance of the SUBJECT
15 PREMISES, I used a portable electronic device to conduct a wireless survey at the front
16 of the SUBJECT PREMISES and discovered numerous Wi-Fi enabled networks. These
17 Wi-Fi networks were all locked. I detected an "xfinitywifi" wireless internet network in
18 the area. Based on my training and experience, I know that Comcast deployed a series of
19 wireless "hotspot" networks for their customers. Comcast accomplished this by
20 providing their wireless internet customers with updated wireless routers capable of
21 broadcasting an additional wireless network. These wireless "hotspot" networks are
22 recognized by the connecting device as "xfinitywifi". Comcast customers can access
23 "xfinitywifi" networks by logging in with their unique Comcast email or username and
24 previously created password. Of particular importance is that the "xfinitywifi" networks
25 are completely separate from the Comcast customer's private home wireless network(s).
26 While conducting a prior investigation, an official with Comcast confirmed with me that
27 Comcast's "xfinitywifi" wireless networks are not linked or connected to the Comcast
28 subscriber's internet service.

27. Any other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, for example, a consent search, could result in an unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a consent-based interview with DIAZ, or any other resident(s) or occupant(s) of the SUBJECT PREMISES, they could rightfully refuse to give consent and the P2P user who distributed child pornography files from a computer at the SUBJECT IP ADDRESS could arrange for destruction of all evidence of the crime before agents could return with a search warrant. Based on my knowledge, training and experience, the only effective means of collecting and preserving the required evidence in this case is through a search warrant. Based on my knowledge, no prior search warrant has been obtained to search the SUBJECT PREMISES.

28. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual user by account and ISP (as described above). When an individual is using the Internet,

1 the individual's IP address is visible to administrators of websites they visit. Further, the
2 individual's IP address is broadcast during most Internet file and information exchanges
3 that occur.

4 29. Based on my training and experience, I know that most ISPs provide only
5 one IP address for each residential subscription. I also know that individuals often use
6 multiple digital devices within their home to access the Internet, including desktop and
7 laptop computers, tablets, and mobile phones. A device called a router is used to connect
8 multiple digital devices to the Internet via the public IP address assigned (to the
9 subscriber) by the ISP. A wireless router performs the functions of a router but also
10 includes the functions of a wireless access point, allowing (wireless equipped) digital
11 devices to connect to the Internet via radio waves, not cables. Based on my training and
12 experience, today many residential Internet customers use a wireless router to create a
13 computer network within their homes where users can simultaneously access the Internet
14 (with the same public IP address) with multiple digital devices.

15 30. Based on my training and experience and information provided to me by
16 computer forensic agents, I know that data can quickly and easily be transferred from one
17 digital device to another digital device. Data can be transferred from computers or other
18 digital devices to internal and/or external hard drives, tablets, mobile phones, and other
19 mobile devices via a USB cable or other wired connection. Data can also be transferred
20 between computers and digital devices by copying data to small, portable data storage
21 devices including USB (often referred to as "thumb") drives, memory cards (Compact
22 Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

23 31. As outlined above, residential Internet users can simultaneously access the
24 Internet in their homes with multiple digital devices. Also explained above is how data
25 can quickly and easily be transferred from one digital device to another through the use
26 of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage
27 devices (USB drives, memory cards, optical discs). Therefore, a user could access the
28 Internet using their assigned public IP address, receive, transfer or download data, and

1 then transfer that data to other digital devices which may or may not have been connected
2 to the Internet during the date and time of the specified transaction.

3 32. Based on my training and experience, I have learned that the computer's
4 ability to store images and videos in digital form makes the computer itself an ideal
5 repository for child pornography. The size of hard drives used in computers (and other
6 digital devices) has grown tremendously within the last several years. Hard drives with
7 the capacity of four (4) terabytes (TB) are not uncommon. These drives can store
8 thousands of images and videos at very high resolution.

9 33. Based on my training and experience, collectors and distributors of child
10 pornography also use online resources to retrieve and store child pornography, including
11 services offered by companies such as Google, Yahoo, Apple, and Dropbox, among
12 others. The online services allow a user to set up an account with a remote computing
13 service that provides email services and/or electronic storage of computer files in any
14 variety of formats. A user can set up an online storage account from any computer with
15 access to the Internet. Evidence of such online storage of child pornography is often
16 found on the user's computer. Even in cases where online storage is used, however,
17 evidence of child pornography can be found on the user's computer in most cases.

18 34. As is the case with most digital technology, communications by way of
19 computer can be saved or stored on the computer used for these purposes. Storing this
20 information can be intentional, i.e., by saving an email as a file on the computer or saving
21 the location of one's favorite websites in, for example, "bookmarked" files. Digital
22 information can also be retained unintentionally, e.g., traces of the path of an electronic
23 communication may be automatically stored in many places (e.g., temporary files or ISP
24 client software, among others). In addition to electronic communications, a computer
25 user's Internet activities generally leave traces or "footprints" and history files of the
26 browser application used. A forensic examiner often can recover evidence suggesting
27 whether a computer contains wireless software, and when certain files under investigation
28

1 were uploaded or downloaded. Such information is often maintained indefinitely until
2 overwritten by other data.

3 35. Based on my training and experience, I have learned that producers of child
4 pornography can produce image and video digital files from the average digital camera,
5 mobile phone, or tablet. These files can then be easily transferred from the mobile device
6 to a computer or other digital device, using the various methods described above. The
7 digital files can then be stored, manipulated, transferred, or printed directly from a
8 computer or other digital device. Digital files can also be edited in ways similar to those
9 by which a photograph may be altered; they can be lightened, darkened, cropped, or
10 otherwise manipulated. As a result of this technology, it is relatively inexpensive and
11 technically easy to produce, store, and distribute child pornography. In addition, there is
12 an added benefit to the child pornographer in that this method of production is a difficult
13 trail for law enforcement to follow.

14 36. As part of my training and experience, I have become familiar with the
15 structure of the Internet, and I know that connections between computers on the Internet
16 routinely cross state and international borders, even when the computers communicating
17 with each other are in the same state. Individuals and entities use the Internet to gain
18 access to a wide variety of information; to send information to, and receive information
19 from, other individuals; to conduct commercial transactions; and to communicate via
20 email.

21 37. Based on my training and experience, I know that cellular mobile phones
22 (often referred to as "smart phones") have the capability to access the Internet and store
23 information, such as images and videos. As a result, an individual using a smart phone
24 can send, receive, and store files, including child pornography, without accessing a
25 personal computer or laptop. An individual using a smart phone can also easily connect
26 the device to a computer or other digital device, via a USB or similar cable, and transfer
27 data files from one digital device to another.
28

1 38. As set forth herein and in Attachment B to this Affidavit, I seek permission
2 to search for and seize evidence, fruits, and instrumentalities of the above-referenced
3 crimes that might be found at the SUBJECT PREMISES in whatever form they are
4 found. It has been my experience that individuals involved in child pornography often
5 prefer to store images of child pornography in electronic form. The ability to store
6 images of child pornography in electronic form makes digital devices, examples of which
7 are enumerated in Attachment B to this Affidavit, an ideal repository for child
8 pornography because the images can be easily sent or received over the Internet. As a
9 result, one form in which these items may be found is as electronic evidence stored on a
10 digital device.

11 39. Based upon my knowledge, experience, and training in child pornography
12 investigations, and the training and experience of other law enforcement officers with
13 whom I have had discussions, I know that there are certain characteristics common to
14 individuals who have a sexualized interest in children and depictions of children:

15 a. They may receive sexual gratification, stimulation, and satisfaction
16 from contact with children; or from fantasies they may have viewing children engaged in
17 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
18 visual media; or from literature describing such activity.

19 b. They may collect sexually explicit or suggestive materials in a
20 variety of media, including photographs, magazines, motion pictures, videotapes, books,
21 slides, and/or drawings or other visual media. Such individuals often times use these
22 materials for their own sexual arousal and gratification. Further, they may use these
23 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
24 selected child partner, or to demonstrate the desired sexual acts. These individuals may
25 keep records, to include names, contact information, and/or dates of these interactions, of
26 the children they have attempted to seduce, arouse, or with whom they have engaged in
27 the desired sexual acts.
28

1 c. They often maintain any “hard copies” of child pornographic
2 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
3 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
4 their home or some other secure location. These individuals typically retain these “hard
5 copies” of child pornographic material for many years, as they are highly valued.

6 d. Likewise, they often maintain their child pornography collections
7 that are in a digital or electronic format in a safe, secure and private environment, such as
8 a computer and surrounding area. These collections are often maintained for several
9 years and are kept close by, often at the individual’s residence or some otherwise easily
10 accessible location, to enable the owner to view the collection, which is valued highly.
11 They also may opt to store the contraband in cloud accounts. Cloud storage is a model of
12 data storage where the digital data is stored in logical pools, the physical storage can span
13 multiple servers, and often locations, and the physical environment is typically owned
14 and managed by a hosting company. Cloud storage allows the offender ready access to
15 the material from any device that has an Internet connection, worldwide, while also
16 attempting to obfuscate or limit the criminality of possession as the material is stored
17 remotely and not on the offender’s device.

18 e. They also may correspond with and/or meet others to share
19 information and materials; rarely destroy correspondence from other child pornography
20 distributors/collectors; conceal such correspondence as they do their sexually explicit
21 material; and often maintain lists of names, addresses, and telephone numbers of
22 individuals with whom they have been in contact and who share the same interests in
23 child pornography.

24 f. They generally prefer not to be without their child pornography for
25 any prolonged time period. This behavior has been documented by law enforcement
26 officers involved in the investigation of child pornography throughout the world.

27 40. In addition to offenders who collect and store child pornography, law
28 enforcement has encountered offenders who obtain child pornography from the internet,

1 view the contents and subsequently delete the contraband, often after engaging in self-
2 gratification. In light of technological advancements, increasing Internet speeds and
3 worldwide availability of child sexual exploitative material, this phenomenon offers the
4 offender a sense of decreasing risk of being identified and/or apprehended with quantities
5 of contraband. This type of consumer is commonly referred to as a 'seek and delete'
6 offender, knowing that the same or different contraband satisfying their interests remain
7 easily discoverable and accessible online for future viewing and self-gratification.

8 I know that, regardless of whether a person discards or collects child pornography he/she
9 accesses for purposes of viewing and sexual gratification, evidence of such activity is
10 likely to be found on computers and related digital devices, including storage media, used
11 by the person. This evidence may include the files themselves, logs of account access
12 events, contact lists of others engaged in trafficking of child pornography, backup files,
13 and other electronic artifacts that may be forensically recoverable.

14 41. Given the above-stated facts, and based on my knowledge, training and
15 experience, along with my discussions with other law enforcement officers who
16 investigate child exploitation crimes, I believe that the P2P user who possessed and
17 distributed child pornography files from the SUBJECT IP ADDRESS likely has a
18 sexualized interest in children and depictions of children and that evidence of child
19 pornography is likely to be found on digital media devices, including mobile and/or
20 portable digital devices that belong to this P2P user or to which this P2P user has access.

21 42. Based on my training and experience, and that of computer forensic agents
22 that I work and collaborate with on a daily basis, I know that every type and kind of
23 information, data, record, sound or image can exist and be present as electronically stored
24 information on any of a variety of computers, computer systems, digital devices, and
25 other electronic storage media. I also know that electronic evidence can be moved easily
26 from one digital device to another. As a result, I believe that electronic evidence may be
27 stored on any digital device present at the SUBJECT PREMISES.

1 43. Based on my training and experience, and my consultation with computer
2 forensic agents who are familiar with searches of computers, I know that in some cases
3 the items set forth in Attachment B may take the form of files, documents, and other data
4 that is user-generated and found on a digital device. In other cases, these items may take
5 the form of other types of data - including in some cases data generated automatically by
6 the devices themselves.

7 44. Based on my training and experience, and my consultation with computer
8 forensic agents who are familiar with searches of computers, I believe that if digital
9 devices are found in the SUBJECT PREMISES, there is probable cause to believe that
10 the items set forth in Attachment B will be stored in those digital devices for a number of
11 reasons, including but not limited to the following:

12 a. Once created, electronically stored information (ESI) can be stored
13 for years in very little space and at little or no cost. A great deal of ESI is created, and
14 stored, moreover, even without a conscious act on the part of the device operator. For
15 example, files that have been viewed via the Internet are sometimes automatically
16 downloaded into a temporary Internet directory or "cache," without the knowledge of the
17 device user. The browser often maintains a fixed amount of hard drive space devoted to
18 these files, and the files are only overwritten as they are replaced with more recently
19 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may
20 include relevant and significant evidence regarding criminal activities, but also, and just
21 as importantly, may include evidence of the identity of the device user, and when and
22 how the device was used. Most often, some affirmative action is necessary to delete ESI.
23 And even when such action has been deliberately taken, ESI can often be recovered,
24 months or even years later, using forensic tools.

25 b. Wholly apart from data created directly (or indirectly) by user-
26 generated files, digital devices - in particular, a computer's internal hard drive - contain
27 electronic evidence of how a digital device has been used, what it has been used for, and
28 who has used it. This evidence can take the form of operating system configurations,

1 artifacts from operating systems or application operations, file system data structures, and
2 virtual memory "swap" or paging files. Computer users typically do not erase or delete
3 this evidence, because special software is typically required for that task. However, it is
4 technically possible for a user to use such specialized software to delete this type of
5 information - and, the use of such special software may itself result in ESI that is relevant
6 to the criminal investigation. HSI agents in this case have consulted on computer
7 forensic matters with law enforcement officers with specialized knowledge and training
8 in computers, networks, and Internet communications. In particular, to properly retrieve
9 and analyze electronically stored (computer) data, and to ensure accuracy and
10 completeness of such data and to prevent loss of the data either from accidental or
11 programmed destruction, it is necessary to conduct a forensic examination of the
12 computers. To effect such accuracy and completeness, it may also be necessary to
13 analyze not only data storage devices, but also peripheral devices which may be
14 interdependent, the software to operate them, and related instruction manuals containing
15 directions concerning operation of the computer and software.

16 **VII. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES**

17 45. In addition, based on my training and experience and that of computer
18 forensic agents that I work and collaborate with on a daily basis, I know that in most
19 cases it is impossible to successfully conduct a complete, accurate, and reliable search for
20 electronic evidence stored on a digital device during the physical search of a search site
21 for a number of reasons, including but not limited to the following:

22 a. Technical Requirements: Searching digital devices for criminal
23 evidence is a highly technical process requiring specific expertise and a properly
24 controlled environment. The vast array of digital hardware and software available
25 requires even digital experts to specialize in particular systems and applications, so it is
26 difficult to know before a search which expert is qualified to analyze the particular
27 system(s) and electronic evidence found at a search site. As a result, it is not always
28 possible to bring to the search site all of the necessary personnel, technical manuals, and

1 specialized equipment to conduct a thorough search of every possible digital
2 device/system present. In addition, electronic evidence search protocols are exacting
3 scientific procedures designed to protect the integrity of the evidence and to recover even
4 hidden, erased, compressed, password-protected, or encrypted files. Since ESI is
5 extremely vulnerable to inadvertent or intentional modification or destruction (both from
6 external sources or from destructive code embedded in the system such as a "booby
7 trap"), a controlled environment is often essential to ensure its complete and accurate
8 analysis.

9 b. Volume of Evidence: The volume of data stored on many digital
10 devices is typically so large that it is impossible to search for criminal evidence in a
11 reasonable period of time during the execution of the physical search of a search site. A
12 single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A
13 single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000
14 double-spaced pages of text. Computer hard drives are now being sold for personal
15 computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally,
16 this data may be stored in a variety of formats or may be encrypted (several new
17 commercially available operating systems provide for automatic encryption of data upon
18 shutdown of the computer).

19 c. Search Techniques: Searching the ESI for the items described in
20 Attachment B may require a range of data analysis techniques. In some cases, it is
21 possible for agents and analysts to conduct carefully targeted searches that can locate
22 evidence without requiring a time-consuming manual search through unrelated materials
23 that may be commingled with criminal evidence. In other cases, however, such
24 techniques may not yield the evidence described in the warrant, and law enforcement
25 personnel with appropriate expertise may need to conduct more extensive searches, such
26 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to
27 determine whether it falls within the scope of the warrant.
28

1 46. In this particular case, and in order to protect the third party privacy of
2 innocent individuals residing in the residence, the following are search techniques that
3 will be applied:

4 i. Device use and ownership will be determined through interviews, if
5 possible, and through the identification of user account(s), associated account names, and
6 logons associated with the device. Determination of whether a password is used to lock a
7 user's profile on the device(s) will assist in knowing who had access to the device or
8 whether the password prevented access.

9 ii. Use of hash value library searches.

10 iii. Use of keyword searches, i.e., utilizing key words that are known to be
11 associated with the sharing of child pornography.

12 iv. Identification of non-default programs that are commonly known to be used
13 for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent,
14 Ares, Shareaza, Gnutella, etc.

15 v. Looking for file names indicative of child pornography, such as, PTHC,
16 PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child
17 pornography.

18 vi. Viewing of image files and video files.

19 vii. As indicated above, the search will be limited to evidence of child
20 pornography and will not include looking for personal documents and files that are
21 unrelated to the crime.

22 47. These search techniques may not all be required or used in a particular
23 order for the identification of digital devices containing items set forth in Attachment B
24 to this Affidavit. However, these search techniques will be used systematically in an
25 effort to protect the privacy of third parties. Use of these tools will allow for the quick
26 identification of items authorized to be seized pursuant to Attachment B to this Affidavit,
27 and will also assist in the early exclusion of digital devices and/or files which do not fall
28

1 within the scope of items authorized to be seized pursuant to Attachment B to this
2 Affidavit.

3 48. In accordance with the information in this Affidavit, law enforcement
4 personnel will execute the search of digital devices seized pursuant to this warrant as
5 follows:

6 a. Upon securing the search site, the search team will conduct an initial
7 review of any digital devices/systems to determine whether the ESI contained therein can
8 be searched and/or duplicated on site in a reasonable amount of time and without
9 jeopardizing the ability to accurately preserve the data.

10 b. If, based on their training and experience, and the resources
11 available to them at the search site, the search team determines it is not practical to make
12 an on-site search, or to make an on-site copy of the ESI within a reasonable amount of
13 time and without jeopardizing the ability to accurately preserve the data, then the digital
14 devices will be seized and transported to an appropriate law enforcement laboratory for
15 review and to be forensically copied ("imaged"), as appropriate.

16 c. In order to examine the ESI in a forensically sound manner, law
17 enforcement personnel with appropriate expertise will produce a complete forensic
18 image, if possible and appropriate, of any digital device that is found to contain data or
19 items that fall within the scope of Attachment B of this Affidavit. In addition,
20 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
21 encrypted data to determine whether the data fall within the list of items to be seized
22 pursuant to the warrant. In order to search fully for the items identified in the warrant,
23 law enforcement personnel, which may include investigative agents, may then examine
24 all of the data contained in the forensic image/s and/or on the digital devices to view their
25 precise contents and determine whether the data fall within the list of items to be seized
26 pursuant to the warrant.

27 d. The search techniques that will be used will be only those
28 methodologies, techniques and protocols as may reasonably be expected to find, identify,

1 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
2 this Affidavit.

3 e. If, after conducting its examination, law enforcement personnel
4 determine that any digital device is an instrumentality of the criminal offenses referenced
5 above, the government may retain that device during the pendency of the case as
6 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
7 the chain of custody, and litigate the issue of forfeiture.

8 49. In order to search for ESI that falls within the list of items to be seized
9 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
10 search the following items (heretofore and hereinafter referred to as "digital devices"),
11 subject to the procedures set forth above:

12 a. Any digital device capable of being used to commit, further, or store
13 evidence of the offense(s) listed above;

14 b. Any digital device used to facilitate the transmission, creation,
15 display, encoding, or storage of data, including word processing equipment, modems,
16 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

17 c. Any magnetic, electronic, or optical storage device capable of
18 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
19 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
20 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

21 d. Any documentation, operating logs and reference manuals regarding
22 the operation of the digital device, or software;

23 e. Any applications, utility programs, compilers, interpreters, and other
24 software used to facilitate direct or indirect communication with the device hardware, or
25 ESI to be searched;


26 f. Any physical keys, encryption devices, dongles and similar physical
27 items that are necessary to gain access to the digital device, or ESI; and
28

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

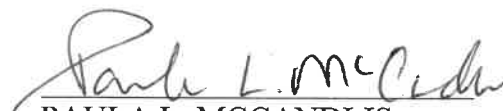
VIII. CONCLUSION

50. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are located at the SUBJECT PREMISES more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. I therefore request that the court issue a warrant authorizing a search of the location, vehicles, and person specified in Attachment A for the items more fully described in Attachment B.

Dated this 17 day of January, 2019.


Toby Ledgerwood, Affiant
Special Agent
Department of Homeland Security
Homeland Security Investigations

SUBSCRIBED and SWORN to before me this 17th day of January, 2019.


PAULA L. MCCANDLIS
United States Magistrate Judge

ATTACHMENT A

Description of Property to be Searched

The SUBJECT PREMISES is the property located at 127 2nd St., Gold Bar, Washington, and is more fully described as a parcel containing a single family house with a basement. The house has white colored siding with white trim around the windows. There is a black mailbox posted in front of the house with the numbers 127 affixed in black lettering with a white background. There are multiple security cameras affixed to the house as well as the entry posts.

The search is to include all rooms within the SUBJECT PREMISES, all persons and vehicles on the SUBJECT PREMISES, all garages, outbuildings, or storage unites, attached or detached, and any digital device(s) found therein.

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media.

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography or evidencing contact with minors;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

- 1 a. Any digital devices and storage device capable of being used to
2 commit, further, or store evidence of the offense listed above;
- 3 b. Any digital devices used to facilitate the transmission, creation,
4 display, encoding or storage of data, including word processing equipment, modems,
5 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;
- 6 c. Any magnetic, electronic, or optical storage device capable of
7 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
8 memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives,
9 camera memory cards, media cards, electronic notebooks, and personal digital assistants;
- 10 d. Any documentation, operating logs and reference manuals regarding
11 the operation of the digital device or software;
- 12 e. Any applications, utility programs, compilers, interpreters, and other
13 software used to facilitate direct or indirect communication with the computer hardware,
14 storage devices, or data to be searched;
- 15 f. Any physical keys, encryption devices, dongles and similar physical
16 items that are necessary to gain access to the computer equipment, storage devices or
17 data; and
- 18 g. Any passwords, password files, test keys, encryption codes or other
19 information necessary to access the computer equipment, storage devices or data;
- 20 8. Evidence of who used, owned or controlled any seized digital device(s) at
21 the time the things described in this warrant were created, edited, or deleted, such as logs,
22 registry entries, saved user names and passwords, documents, and browsing history;
- 23 9. Evidence of malware that would allow others to control any seized digital
24 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
25 as evidence of the presence or absence of security software designed to detect malware;
26 as well as evidence of the lack of such malware;
- 27 10. Evidence of the attachment to the digital device(s) of other storage devices
28 or similar containers for electronic evidence;

1 11. Evidence of counter-forensic programs (and associated data) that are
2 designed to eliminate data from a digital device;

3 12. Evidence of times the digital device(s) was used;

4 13. Any other ESI from the digital device(s) necessary to understand how the
5 digital device was used, the purpose of its use, who used it, and when.

6 14. Records and things evidencing the use of the IP address 67.183.169.49 (the
7 SUBJECT IP ADDRESS) including:

8 a. Routers, modems, and network equipment used to connect
9 computers to the Internet;

10 b. Records of Internet Protocol (IP) addresses used;

11 c. Records of Internet activity, including firewall logs, caches, browser
12 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
13 entered into any Internet search engine, and records of user-typed web addresses.

14
15 **The seizure of digital devices and/or their components as set forth herein is**
16 **specifically authorized by this search warrant, not only to the extent that such**
17 **digital devices constitute instrumentalities of the criminal activity described above,**
18 **but also for the purpose of the conducting off-site examinations of their contents for**
19 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
20
21
22
23
24
25
26
27
28